(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 293 554 (13) A1
(43) 17.12.1998

(12)

(21) 2 293 554

(22) 03.06.1998

(51) Int. Cl.[7]: H04Q 007/32

(85) 10.12.1999

(86) PCT/DE98/01516

(87) WO98/57510

(30) 197 24 901.9 DE 12.06.1997

(71) SIEMENS NIXDORF INFORMATIONSSYSTEME AG, Heinz-Nixdorf-Ring 1, PADERBORN, XX (DE).

(72) WIEHLER, GERHARD (DE).

(74) FETHERSTONHAUGH & CO.

(54) APPAREIL UTILISE DANS LA TECHNIQUE DE TELECOMMUNICATION ET/OU DE TELECOMMANDE POURVU D'UNE UNITE A CARTE A PUCE, DE TELS APPAREILS A ORDINATEUR COUPLE POUR DES UTILISATION INTERNET OU RESEAU

(54) TELECOMMUNICATION AND/OR REMOTE CONTROL DEVICE WITH A CHIP CARD UNIT, SAME DEVICE WITH A COUPLED COMPUTER FOR INTERNET OR NETWORK APPLICATIONS

(57)

A chip card unit (13) pertaining to a mobile radio telephone, for instance, is connected to an interface (12) for a computer via a control unit (11) enabling the mobile radio telephone (10) to operate as a card terminal when coupled to a computer (30). When the computer (30) is connected to a telecommunication network (40), occupation of network services by service providers (50) is also possible. Chip card applications include mutual client-server authentication, verification of access rights, digital signature for sensitive data, generation of keys to encrypt data, proof of ordering, payment from an electronic purse, etc.

OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

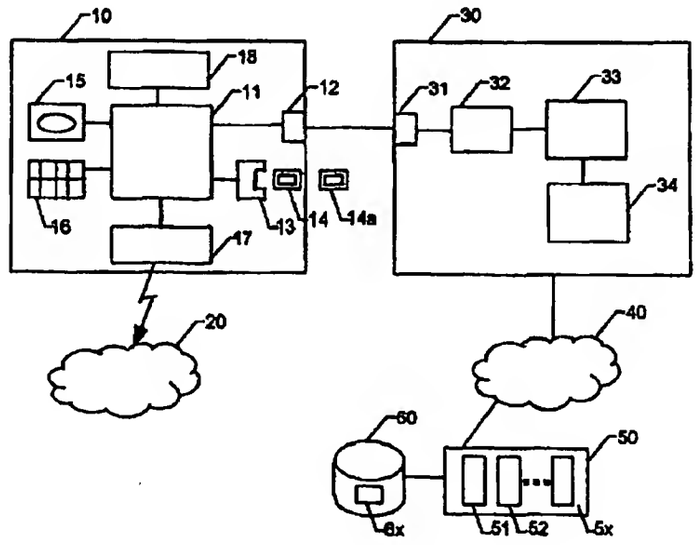
(21) (A1) **2,293,554**
(86) 1998/06/03
(87) 1998/12/17

(72) WIEHLER, GERHARD, DE
(71) SIEMENS NIXDORF INFORMATIONSSYSTEME AG, DE

(51) Int.Cl.[7] H04Q 7/32
(30) 1997/06/12 (197 24 901.9) DE

(54) **APPAREIL UTILISE DANS LA TECHNIQUE DE TELECOMMUNICATION ET/OU DE TELECOMMANDE POURVU D'UNE UNITE A CARTE A PUCE, DE TELS APPAREILS A ORDINATEUR COUPLE POUR DES UTILISATION INTERNET OU RESEAU**

(54) **TELECOMMUNICATION AND/OR REMOTE CONTROL DEVICE WITH A CHIP CARD UNIT, SAME DEVICE WITH A COUPLED COMPUTER FOR INTERNET OR NETWORK APPLICATIONS**



(57) L'invention concerne le raccordement d'une unité à carte à puce (13) par exemple d'un radiotéléphone mobile (10), en tant qu'appareil, par l'intermédiaire d'une unité de commande (11), à l'interface de raccordement (12) destinée à un ordinateur (30), le dit raccordement permettant d'utiliser ledit radiotéléphone

(57) A chip card unit (13) pertaining to a mobile radio telephone, for instance, is connected to an interface (12) for a computer via a control unit (11) enabling the mobile radio telephone (10) to operate as a card terminal when coupled to a computer (30). When the computer (30) is connected to a telecommunication network (40),

OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(21) (A1) **2,293,554**
(86) 1998/06/03
(87) 1998/12/17

mobile (10), lorsqu'il est couplé avec un ordinateur (30), comme terminal à carte. Si l'ordinateur (30) est connecté à un réseau de communication (40), l'occupation des services de réseau par des prestataires de service (50) est également possible. La carte à puce peut être utilisée, par exemple, pour l'authentification mutuelle client-serveur, pour la vérification de droits d'accès, pour la signature numérique de données sensibles, pour la production de clés servant au criptage de données, pour l'apport de la preuve d'un processus de commande, pour le paiement à partir d'un porte-monnaie électronique etc..

occupation of network services by service providers (50) is also possible. Chip card applications include mutual client-server authentication, verification of access rights, digital signature for sensitive data, generation of keys to encrypt data, proof of ordering, payment from an electronic purse, etc.

Abstract

Mobile Radio Terminal with Coupled Computer for Internet or Network Applications and a Method for Operating such a Combination of Equipment

Connection of the chip card unit 13, e.g., of a mobile radio telephone 10 as an apparatus by way of a control unit 11 to the connection interface 12 for a computer 30, so that the mobile radio telephone 10 can be operated as a card terminal when connected to a computer 30. If the computer 30 is connected to a communications network 40, it is then possible to use network services made available by a service provider 50. Chip card applications, e.g., for mutual client-server authentication, for verification of access rights, for appending a digital signature to sensitive data, for generating keys for encoding data, and for proving an ordering process, and for making payments from an electronic purse, etc.

Figure 1

Mobile Radio Terminal with Coupled Computer for Internet or Network Applications and a Method for Operating such a Combination of Equipment

The present invention relates to arrangements and methods for using services offered on the Internet or other networks, which require a high level of security. Examples of apparatuses with chip-card units are mobile radio telephones that are essentially used for transmitting speech over mobile radio networks. The so-called SIM module that is integrated into the mobile radio telephone or the integrated chip card are used to authenticate the mobile radio telephone as an apparatus that is authorised for mobile radio and includes a key for encoding the speech information that is transmitted, or for decoding the speech information that is received.

Another type of apparatus with chip card units includes, for example, remote controls for television sets, in which the chip card is used as proof of authorisation for receiving pay-for-view television programmes and, optionally, as a means for making payments.

Computers, such as personal computers or laptops, that have a connection to a fixed network or a mobile network can use Internet applications by means of the http protocol. In the case of procedures in which security is particularly relevant, such as, for example, in the case of placing orders or making

payments, chip cards are used to control the particular transactions by way of a chip-card reader that is connected to the computer. Connection can also be made to a mobile radio network by way of a mobile radio telephone that is equipped with a data connection; see, for example, *PC Professional*, March, 1994, pp. 253-260, or *Cash Flow*, 2/95, pp. 140-141.

In this connection, it is known from WO 96/25828 that when a computer is connected to a mobile radio network by way of a mobile radio telephone, using an appropriate chip card for the mobile radio telephone, services that are available on the computer and selected by way of the identification code can be controlled after inputting an identification code by way of the mobile radio telephone.

In addition, it is known from DE 195 38 842 A1 that configuration or speech-subscriber data can be transmitted by way of the data connection to the mobile radio telephone to a memory in the mobile radio telephone, when it is also possible to use the memory on the subscriber-card chip. In the same way, this data that is stored in the mobile radio telephone can be read and amended in the computer connected to it in this way.

Also known are combinations of apparatuses made up of television receivers and computers, in which one display is used jointly by the television section and the computer section.

Examples of possible applications involving a computer combined with the chip card are authentication, generation of digital signatures, credit/debit card transactions, and electronic purse transactions.

A particularly high a level of security can be achieved by asymmetric cryptographic methods in which the private key is stored in the chip cards in such a way that it cannot be read out, and the corresponding crypto processes can be carried out in the chip card so that they cannot be manipulated. Chip card components for applications of this kind are already available on the market; one example of such a component is the SLE 44CR80S, which is manufactured by Siemens AG.

It is the objective of the present invention to so broaden the range of application of apparatuses and with chip card units such that secure transactions are possible in conjunction with a computer.

According to Claim 1, this has been achieved in that a mobile radio terminal apparatus is so expanded by using an appropriate chip card that it can also be used as a card terminal for a computer. The use of a mobile radio terminal modified in this way, in conjunction with a computer that is connected to it and which is connected in the manner known per se to a communications network, makes it possible to use personal or public network

services that require a high level of security by way of the Internet, without the computer having to have a chip card reader. This results in a major advantage for mobile radio telephone owners in that they can use network services from any type of standard computer, regardless of location.

Developments of the present invention relate to methods used to operate such a combination of apparatuses. These apply, amongst other things, to activating the mobile radio terminal used as a card terminal and which, in addition to using network services in the usual manner, also permits encoding and decoding in the manner known per se.

Particular advantages result from the fact that highly sensitive data, such as personal identification numbers (PIN) and sums of money can be input at the mobile radio terminal using the keypad and, given an available display, can be shown unencoded before they are coded and passed on to the computer. This avoids having to use the computer keyboard for input, so that viruses that may be resident in the computer cannot falsify the data that is input.

It is also an advantage that control words can be input by way of a microphone and used as proof of authorisation; these words and then digitized and transferred to a control section of the communications network, where they are compared with a reference

the basis of a personal biometric feature, which is in keeping with the increased demands for security.

In addition, data and/or control information can be transmitted through the connection interface to the memory in the mobile radio terminal, where it can be stored. Thus, it is possible to modify or store data on the chip card. Such data can, for example, be keys for encoding or decoding, or can be a sum of money for a cashcard. The latter provides the possibility of a card telephone when, if it is used as a telephone, incoming fee pulses can deduct the appropriate amount of money in each particular instance.

Details of present invention are described in greater detail below on the basis of one embodiment that shown in the drawings are appended in hereto. These drawings show the following:

Figure 1: a schematic overview of a computer with a connection to a network and a connected mobile radio telephone as a card terminal, for using network services;

Figure 2: a schematic representation of a chip card used for various applications.

Figure 1 shows a mobile radio telephone 10 as an apparatus with the chip card unit, this being connected by way of a standard interface 12, e.g., an RS 232 interface, to a computer 30 that is

interface 12, e.g., an RS 232 interface, to a computer 30 that is a conventional PC. Within the mobile radio telephone 10, the interface 12 is connected to a control unit 11 to which a contacting unit 13 for the SIM module/the chip card 14/14a, a display 15, the keypad 16, a speech and radio module 17, as well as a memory 18 are also connected. The speech and radio module 17 has access to the mobile radio network 20 in the usual way.

Only the interface 31 for the mobile radio telephone 10 with the associated driver 32, which are part of the computer 30, are shown, together with the so-called browser 32 and computer applications 34 for using network services, for example, the Internet; these are connected by way of the communications network 40 to an appropriate provider 50, e.g., in the form of the so-called server.

The applications that are accessible with a key are stored on the SIM module or the chip card 14, 14a. Individual chip cards can be provided for the various applications. However, as is shown in Figure 2, the mobile radio applications for GSM/DCS 141 as well as the various Internet/network applications 142, 143, 14x can be stored on a chip card with their various keys.

Before using one of the network services, an appropriate chip card is to be selected and inserted into the contacting unit 13 of the mobile radio telephone 10 that is coupled to the computer

telephone 10 as a card terminal is to be loaded with the appropriate driver software by way of the connecting interface 31. This can be done from a diskette. However, in order to prevent manipulation at the driver 32, it is expedient that the driver software--signed with a private key by the mobile radio network operator--be loaded from an appropriate server on demand from the computer 30 and loaded into the driver 32 by way of the communications network. Subsequently, verification of the driver software can be effected automatically on the basis of a corresponding public key of the mobile radio network operator located in an application area, e.g., 14x, on the chip card 14/14a.

It is expedient that the driver software operate according to an established standard, such as ISO 7816-3 and the ICC specification developed jointly by the PC/SC workgroup and Microsoft (http//:smartcardsys.com).

The network application can be started within the computer 30, for example, by calling up the browser 33 and inputting a so-called "Uniform Resource Locator" (URL). This establishes a connection to the service provider 50 by way of the network 40, when the desired services 51, 52, ..., 5x can then be used. The mobile radio telephone 10 or the control unit 11 that is connected then acts as a conventional card terminal. Depending on the services 51, 52, ..., 5x that are available from the service

the services 51, 52, ..., 5x that are available from the service provider, chip card applications 142, 143, .., 14x can be selected and used, for example, for mutual client-service authentication, for verification of access rights, for providing digital signatures for sensitive data, for the generation of keys for encoding data, for proof of ordering, and for payment from an electronic purse.

As compared to a conventional chip card reader, the present invention permits additional functions that ensure a considerably higher level of security:

In principle, computers that are connected to the Internet are exposed to imported viruses. For example, a sum of money that is to be transferred between accounts and which is input by way of the computer keyboard can be falsified by such a virus before the transaction can concluded correctly with the Internet server.

If the mobile radio telephone or another apparatus is used as a card terminal, this manipulation can be prevented in that--as a result of the computer/server application--sensitive data such as the sum to be transferred is input by way of the keypad 16 on the apparatus 10. The control unit 11 is informed of this amount by way of a code, so that the data that is input can, on the one hand, be shown unencoded on the display 15, where it can be checked. On the other hand, this data is encoded or signed by a

chip card application 14x, and then transferred to the computer 30 or the responsible server for further processing.

In the same way, in the event that a PIN number required by a computer/network application is input, the PIN that is input by way of the keypad 16 is encoded in the chip card before it is passed on to the computer/network application.

Applications that require a high level of security frequently require authentication that is based on biometric features. Using the present invention as described herein, this can be done in the following way:

After successful, mutual client-server authentication based on asymmetric crypto methods, the user, as the so-called client, is required to provide a speech sample, e.g., an agreed upon recognition word, which is spoken three times, one after the other, into the microphone 17 of the mobile radio telephone 10. Then, the control unit 11, triggered for example by a control code transmitted from the application 5x or from the browser 33, passes the digitised flow of speech to the responsible application, e.g., 5x, in the form of a bit string. This extracts the personal speech features from the bit string that has been received, and compares these with reference patterns 6x stored on the hard disk 60 in order to verify the identity of the user on the basis of his speech sample.

The present invention also makes provisions such that within the framework of a computer application 34, data such as telephone lists, address lists, sale dates, price lists, etc., can be loaded into the memory 18 of the mobile radio telephone and can be shown on the display 15, with selection also being possible by way of the keypad 16.

In another computer application 34, digitised data that is keyed in or input by voice at the mobile radio telephone 10 can be transferred into the computer 30 and further processed either there or in a network server, or else subsequently recalled by other users.

In addition, it is also possible for programmes to be loaded into the memory 18 of the mobile radio telephone 10 by way of the connection interface 31/12 as a result of a command from a computer application 34; these can then be run--separated by time--in the control unit 11.

Finally, applications/keys can be modified, erased, or loaded on the chip card itself as a result of a command from a computer application 34.

In all cases, data, programmes, or applications can be transferred between the mobile radio telephone 10 or the chip card 14/14a and the computer 30 or the network server either

encoded or so that their integrity is secured. The keys required to do this are either already stored on the chip card or were exchanged previously between the computer/network server application and the chip card, e.g., by using the Diffy-Hellman method. Furthermore, the mobile radio telephone 10 can generally be used in a similar manner for encoding or decoding data.

A further version of the present invention is the general use of a chip card application in GSM and fixed networks. An example of this is the electronic purse. It can be loaded, for example, as application 14x on the chip card 14/14a installed in the mobile radio telephone 10, by way of a computer/network application 33/34/5x and then decremented according to long-distance tariffs during a subsequent GSM telephone conversation, e.g., by a pulse emitted by the radio exchange at regular time intervals. This sort of "pre-paid" telephoning reduces the risk of fraud to which the users of mobile radio are exposed today. The same thing applies to any other apparatus that is comparably equipped with chip card units, e.g., remote controls that are used in connection with pay-for-view television.

Patent Claims

1. Mobile radio terminal (10) with the chip card unit (13) for a chip card (14, 14a) as proof of authorisation for a user and devices (12) for connection to a computer (30), the mobile radio terminal apparatus (10) being used as a card terminal for the computer (30) for authentication and proof of authorisation when services that are available on the computer are accessed when an appropriate chip card (14a) is used, characterised in that the computer (30) is connected to a communications network (40) independently of the mobile radio terminal apparatus (10); and in that the mobile radio terminal apparatus (10) can be used as a connected card terminal within the communications network (40) for accessing network services.

2. Mobile radio terminal apparatus as defined in Claim 1, characterised in that all the components that are available for using the mobile radio terminal apparatus (10) are connected with a control unit (11) so that input by way of the keypad (16) or a microphone can either be stored or passed on by way of the interface (12), or that data that arrives by way of the interface (12) can be stored and/or shown on a display (15), the data that is to be shown being selectable by way of the keypad (16).

3. Method for operating a combination of equipment consisting of a mobile telephone terminal apparatus (10) with chip card unit (13) for a chip card (14, 14a) as proof of authorisation for the user, and the computer (30) that is connected to the mobile radio terminal apparatus (10), the mobile radio terminal apparatus (10) being usable as a card terminal for the computer (30) to authenticate and provide proof of authorisation for using the services that are available on the computer when the appropriate chip cards (14a) are used, characterised in that the computer (30) is connected to a communications network (40) independently of the mobile radio terminal apparatus (10); and in that prior to the use of a network service that requires a card terminal in the communications network (40) a driver (32) that controls a computer interface (31) for connecting the mobile radio terminal apparatus (10) to the computer (30) is first loaded with the required driver software.

4. Method as defined in Claim 3, characterised in that the provision of the driver software is effected by a request signed by an application (e.g., 14x) on the chip card (14, 14a).

5. Method as defined in Claim 3 or Claim 4, characterised in that the driver software is loaded into the driver (32) of the computer (30) from the server of the mobile radio

network operator by way of the communications network (40) on demand; and in at the presence of the authentic driver software is automatically checked on the basis of the driver software being signed with a private key in conjunction with the associated public key on the chip card (14/14a).

6. Method as defined in one of the Claims 3 to 5, characterised in that once a connection has been established from the computer (30) through the communications network (40) to a service provider (50), chip card applications can be both selected and executed using the mobile radio terminal apparatus (10) as a card terminal.

7. Method as defined in Claim 6, characterised in that as a card terminal for the computer (30), the mobile radio terminal apparatus (10) can be used to encode sensitive data.

8. Method as defined in Claim 6 or Claim 7, characterised in that highly sensitive data such as PIN numbers or sums of money that are required within the framework of a running application can be input from the keypad (16) of the mobile radio terminal apparatus (10) and then passed on in encoded form from the control unit (11) in conjunction with the chip card (14, 14a).

9. Method as defined in Claim 6 or Claim 7, characterised in that check words that are input by way of a microphone can be passed to the control element of the application that has been opened in order that the user can be authenticated in conjunction with reference patterns that are stored in memory.

10. Method as defined in one of the Claims 6 to 9, characterised in that data accepted from the computer within the framework of an application is passed to the memory (18) of the mobile radio terminal apparatus (10).

11. Method as defined in Claim a 10, characterised in that data transferred from the computer (30) serves to modify data in a chip of the chip card (14, 14a).

12. Method as defined in Claim 11, characterised in that in the case of a chip card (14, 14a) that serves as a cash card, the amount pulses that arrive during radio connection of the mobile radio terminal apparatus (10) deduct the appropriate sum of money.

Fetherstonhaugh & Co.
Ottawa, Canada
Patent Agents

1/1

FIG 1

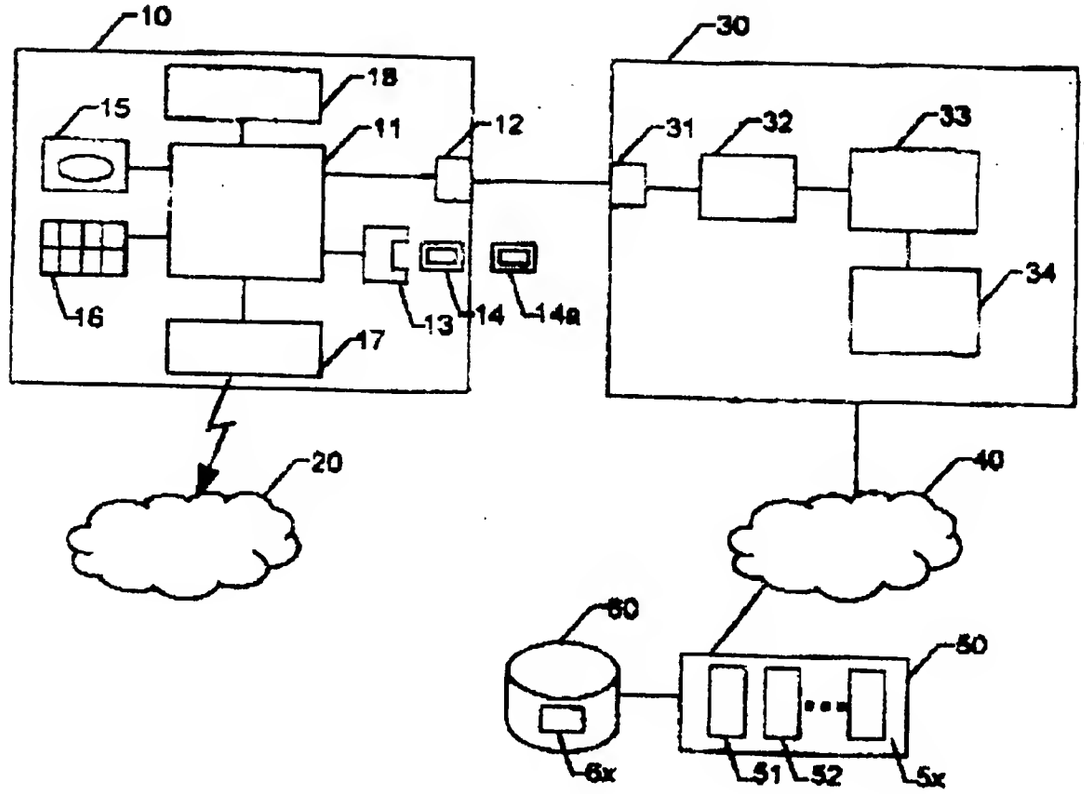
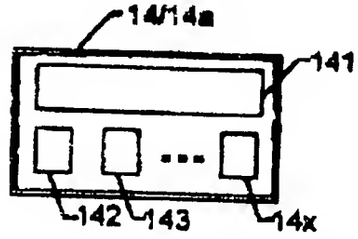

10
18
15
11
12
30
31
32
33
34
16
13
14
14a
17
20
40
60
50
6x
51
52
5x

FIG 2


14/14a
141
142
143
14x